CLAIMS

SUB C1 1. A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a user defined read list containing user identifications that are allowed to read a specified set of attributes;

providing a system administrator defined read access control command;

said read access control command listing the user attributes that said administrator has selected for user defined read access; and

said read access control command referring to said user defined read list thereby allowing said read user identifications read access to said user attributes.

2. The process of Claim 1, wherein upon a client read access, the directory server selects a specific read access control command according to the attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

3. The process of Claim 1, further comprising the steps of:

providing a user defined write list containing user identifications that are allowed to write a specified set of attributes;

providing a system administrator defined write access control command;

said write access control command listing the user attributes that said administrator has selected for user defined write access; and

said write access control command referring to said user defined write list thereby allowing said write user identifications write access to said user attributes.

4. The process of Claim 3, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

SUB C2 5. A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a system administrator defined read access control command that lists the user attributes that said administrator has selected for user defined read access;

providing a system administrator defined write access control command that lists the user attributes that said administrator has selected for user defined write access;

providing a plurality of user defined read lists containing user identifications that are allowed to read said user attributes that said administrator has selected for user defined read access; and

providing a plurality of user defined write lists containing user identifications that are allowed to write said user attributes that said administrator has selected for user defined write access;

wherein when a client read access to one of the user attributes that said administrator has selected for user defined read access occurs, said read access control command and the read list of the owner of the attribute being accessed are used to determine if said client has permission to execute said read access; and

wherein when a client write access to one of the user attributes that said administrator has selected for user defined write access occurs, said write access control command and the write list of the owner of the attribute being accessed are used to determine if said client has permission to execute said write access.

6. A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a user defined write list containing user identifications that are allowed to write a specified set of attributes;

providing a system administrator defined write access control command;

said write access control command listing the user attributes that said administrator has selected for user defined write access; and

said write access control command referring to said user defined write list thereby allowing said write user identifications write access to said user attributes.

7. The process of Claim 6, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

8. The process of Claim 6, further comprising the steps of:

providing a user defined read list containing user identifications that are allowed to read a specified set of attributes; and

providing a system administrator defined read access control command;

wherein said read access control command lists the user attributes that said administrator has selected for user defined read access; and

wherein said read access control command refers to said user defined read list thereby allowing said read user identifications read access to said user attributes.

9. The process of Claim 8, wherein upon a client read access, the directory server selects a specific read access control command according to the attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

SubC37

10. An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:

a user defined read list containing user identifications that are allowed to read a specified set of attributes; and

a system administrator defined read access control command;

wherein said read access control command lists the user attributes that said administrator has selected for user defined read access; and

wherein said read access control command refers to said user defined read list thereby allowing said read user identifications read access to said user attributes.

11. The apparatus of Claim 10, wherein upon a client read access, the directory server selects a specific read access control command according to the attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

12. The apparatus of Claim 10, further comprising:

a user defined write list containing user identifications that are allowed to write a specified set of attributes; and

a system administrator defined write access control command;

wherein said write access control command lists the user attributes that said administrator has selected for user defined write access; and wherein said write access control command refers to said user defined write list thereby allowing said write user identifications write access to said user attributes.

13. The apparatus of Claim 12, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

SUB C4>

~~14. An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:~~

~~a system administrator defined read access control command that lists the user attributes that said administrator has selected for user defined read access;~~

~~a system administrator defined write access control command that lists the user attributes that said administrator has selected for user defined write access;~~

~~a plurality of user defined read lists containing user identifications that are allowed to read said user attributes that said administrator has selected for user defined read access; and~~

~~a plurality of user defined write lists containing user identifications that are allowed to write said user attributes that said administrator has selected for user defined write access;~~

~~wherein when a client read access to one of the user attributes that said administrator has selected for user defined read access occurs, said read access control command and the read list of the owner of the attribute being accessed are used to determine if said client has permission to execute said read access; and~~

~~wherein when a client write access to one of the user attributes that said administrator has selected for user defined write access occurs, said write access control command and the write list of the owner of the attribute being accessed are used to determine if said client has permission to execute said write access.~~

~~15. An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:~~

~~a user defined write list containing user identifications that are allowed to write a specified set of attributes; and~~

~~a system administrator defined write access control command;~~

~~wherein said write access control command lists the user attributes that said administrator has selected for user defined write access; and~~

wherein said write access control command refers to said user defined write list thereby allowing said write user identifications write access to said user attributes.

16. The apparatus of Claim 15, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

17. The apparatus of Claim 15, further comprising:

a user defined read list containing user identifications that are allowed to read a specified set of attributes;

a system administrator defined read access control command;

wherein said read access control command lists the user attributes that said administrator has selected for user defined read access; and

wherein said read access control command refers to said user defined read list thereby allowing said read user identifications read access to said user attributes.

18. The apparatus of Claim 17, wherein upon a client read access, the directory server selects a specific read access control command according to the attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

Sub C57 19. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a user defined read list containing user identifications that are allowed to read a specified set of attributes;

providing a system administrator defined read access control command;

said read access control command listing the user attributes that said administrator has selected for user defined read access; and

said read access control command referring to said user defined read list thereby allowing said read user identifications read access to said user attributes.

20. The method of Claim 19, wherein upon a client read access, the directory server selects a specific read access control command according to the attribute being accessed

and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

21. The method of Claim 19, further comprising the steps of:

providing a user defined write list containing user identifications that are allowed to write a specified set of attributes;

providing a system administrator defined write access control command;

said write access control command listing the user attributes that said administrator has selected for user defined write access; and

said write access control command referring to said user defined write list thereby allowing said write user identifications write access to said user attributes.

22. The method of Claim 21, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

SUB C6

~~23. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:~~

~~providing a system administrator defined read access control command that lists the user attributes that said administrator has selected for user defined read access;~~

~~providing a system administrator defined write access control command that lists the user attributes that said administrator has selected for user defined write access;~~

~~providing a plurality of user defined read lists containing user identifications that are allowed to read said user attributes that said administrator has selected for user defined read access;~~

~~providing a plurality of user defined write lists containing user identifications that are allowed to write said user attributes that said administrator has selected for user defined write access;~~

~~wherein when a client read access to one of the user attributes that said administrator has selected for user defined read access occurs, said read access control command and the read list of the owner of the attribute being accessed are used to determine if said client has permission to execute said read access; and~~

wherein when a client write access to one of the user attributes that said administrator has selected for user defined write access occurs, said write access control command and the write list of the owner of the attribute being accessed are used to determine if said client has permission to execute said write access.

24. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a user defined write list containing user identifications that are allowed to write a specified set of attributes;

providing a system administrator defined write access control command;

said write access control command listing the user attributes that said administrator has selected for user defined write access; and

said write access control command referring to said user defined write list thereby allowing said write user identifications write access to said user attributes.

25. The method of Claim 24, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

26. The method of Claim 24, further comprising the steps of:

providing a user defined read list containing user identifications that are allowed to read a specified set of attributes; and

providing a system administrator defined read access control command;

wherein said read access control command lists the user attributes that said administrator has selected for user defined read access; and

wherein said read access control command refers to said user defined read list thereby allowing said read user identifications read access to said user attributes.

27. The method of Claim 26, wherein upon a client read access, the directory server selects a specific read access control command according to the attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.